Listing of Claims:

This listing of claims is provided for the Examiner's convenience and will replace all prior versions, and listings, of claims in the application. No claims are amended.

1. (Previously Presented) A method for detecting ARP spoofing in a computer network, the method comprising:

receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and

analyzing at least one association in a database accessible to the ARP collector to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association, and wherein the at least one association includes a MAC address that is identical to the MAC address included in the data packet.

2. (Previously Presented) The method of claim 1, wherein the data packet is encrypted by the first device.

3. (Canceled)

4. (Previously Presented) The method of claim 1, wherein the at least one association includes a time at which an associated ARP reply was received on a port.

5. (Previously Presented) The method of claim 4, wherein the at least one association further includes an identification of the port.

6. (Previously Presented) The method of claim 1, wherein if it is determined that there is a spoofed ARP reply, blocking a port on which the spoofed ARP reply was received.

7. (Previously Presented) The method of claim 1, wherein if it is determined that there is a spoofed ARP reply, filtering a MAC address which generated the spoofed ARP reply at a port at which the spoofed ARP reply was received.

8. (Previously Presented) The method of claim 1 further comprising:
transmitting the data packet to the ARP collector; and
generating an alert if an ARP spoofing condition occurs.

9 - 14. (Canceled)

15. (Previously Presented) A device for storing and analyzing ARP information to detect ARP spoofing, the device including:

an interface for receiving packets, wherein the packets include ARP reply information, including information identifying a port on a network device where an ARP reply was received;

a processor coupled to the interface, and programmed to analyze a first received packet, and to identify a first MAC address which is identified as a source MAC address for a first ARP reply, and to identify a first IP address which is identified as a source IP address for the first ARP reply, and to identify a first port on which the first ARP reply was received;

a database coupled to the processor, and which stores information from the packets, wherein for the first packet received at the interface, the database stores the first MAC address, the first IP address, and the port on which the first ARP reply was received; and

wherein the processor is further operable to analyze information in the database and information in a received packet to identify whether a spoofed ARP reply has been transmitted by a host, the analyzing being based upon a time associated with at least one entry stored in the database, the at least one entry including a MAC address that is identical to a MAC address included in the received packet.

16. (Original) The device of claim 15, further including a garbage collection timer module which determines when ARP reply information is stale and should be cleared from

the database.

17. (Previously Presented) The device of claim 15, wherein processor is further operable to generate an alert if a spoofed ARP reply has been detected.

18. (Original) The device of claim 15, wherein the processor is further operable, to identify a port on which a spoofed ARP reply has been received and to generate a signal which causes the port to be blocked in response to identifying the port on which the spoofed ARP reply has been received.

19. (Original) The device of claim 15, wherein the processor is further operable to identify a port on which a first spoofed ARP reply has been received and to identify a MAC address of an attacking host which generated the spoofed ARP reply, and in response to identifying the port, and the MAC address of the attacking host, the processor generates a signal which indicates that the MAC address should be MAC filtered at the port.

20. (Previously Presented) A method for detecting ARP spoofing in a computer network, the method comprising:

receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and

analyzing at least two associations in a database accessible to the ARP collector to determine whether ARP spoofing occurs, wherein each of the at least two associations include a MAC address that is identical to the MAC address included in the data packet.

21. (Previously Presented) The method of claim 1, wherein the MAC address and the IP address included in the data packet are stored as part of a first association in the

database, wherein the first association includes a first time, and wherein analyzing at least one association in the database comprises:

identifying a second association in the database, wherein the second association includes a MAC address that is identical to the MAC address of the first association, an IP address that is identical to the IP address of the first association, and a second time;

identifying a third association in the database, wherein the third association includes a MAC address that is identical to the MAC address of the first association, an IP address that is different from the IP address of the first association, and a third time subsequent to the second time; and

determining whether ARP spoofing occurs based on whether the first, second, and third times fall within a predefined time interval.

22. (Previously Presented) A network device comprising:

a database;

one or more ports; and

a processing component configured to:

receive a data packet generated by another network device, the data packet including a MAC address and a source IP address from an ARP reply; and

analyze at least one association in the database to determine whether the ARP reply is a spoofed ARP reply, wherein the analyzing is based on a time associated with the at least one association, and wherein the at least one association includes a MAC address that is identical to the MAC address included in the data packet.

23. (Previously Presented) The network device of claim 22, wherein said another network device is a Layer 2 switch.